UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/782,593	02/12/2001	Marc VanHeyningen	05313.00001	9483

7590 06/17/2004

Banner & Witcoff, Ltd.
1001 G Street, N.W.
Washington, DC 20001-4597

EXAMINER	
SON, LINH L D	
ART UNIT	**PAPER NUMBER**
2135	9

DATE MAILED: 06/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/782,593	VANHEYNINGEN, MARC	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 February 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4,5,6,7,and 8*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-3, and 8-9 are rejected under 35 U.S.C. 102(e) as being anticipated by Liao et al, hereinafter "Liao", (US/6148405).

3. As per claim 1, Liao discloses a method of transmitting data securely over a computer network (See the Abstract), comprising the steps of: (1) establishing a communication path between a first computer and a second computer (Col 3 lines 23-57); (2) encrypting and transmitting data records between the first computer (Client's handheld device) and the second computer (Uplink Server, Col 6 lines 12-17 and Col 3 lines 58-67) using an unreliable communication protocol (UDP, Col 6 lines 11-46) wherein each data record is encrypted without reference to a previously transmitted data record (Col 7 line 60 to Col 8 line 15); and (3) in the second computer, receiving and decrypting the data records transmitted in step (2) (Col 3 lines 57-67 and UDP, Col 6 lines 25-30) without

reference to a previously received data record (Col 7 line 60 to Col 8 line 15). The block cipher RC5 algorithm does not encrypt/decrypt the data record using the reference to a previously transmitted/received data record.

4. As per claim 2, Liao discloses the method of claim 1, further comprising the step of, prior to step (1), establishing a reliable communication path between the first computer and the second computer and exchanging security credentials over the reliable communication path (Col 7 lines 6-25).

5. As per claim 3, Liao discloses the method of claim 2, wherein the step of exchanging security credentials comprises the step of exchanging an encryption key that is used to encrypt the data records in step (2) (Col 7 lines 6-25).

6. As per claim 8, Liao discloses the method of claim 1, wherein step (1) is performed using the Transmission Control Protocol, and wherein step (2) is performed using the User Datagram Protocol (UDP, Col 6 lines 25-30).

7. As per claim 9, Liao discloses the method of claim 1, wherein step (2) is performed by a proxy server that encrypts data records received from another server (Col 5 lines 13-17).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 4-7, and 10-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Liao et al, hereinafter "Liao", (US/6148405) in view of Roberts (US2002/0094085A1).

10.

As per claims 4, Liao discloses the method of claim 1. Liao further teaches the method to authenticate a communication session using a combination of nonce and other credential and if successful the transaction data is encrypted using the symmetric key acquired from the session establishment (See Claim 1,2,and 3 rejections). However, Liao does not teach the step (2) comprises the step of incorporating a nonce in each data record that is used by the second computer in combination with a previously shared encryption key to decrypt each of the data records in step (3). Nevertheless, Roberts discloses the "Methods and Systems for Generating encryption Keys using Random bit Generators" invention, which includes the step of incorporating a random seed in each data record that is used by the second in combination with a previously shared encryption key to decrypt each of the data records (Fig. 5, Para 0083). By definition of the Nonce, the random seed is also interpreted is the nonce. Further, Roberts does teach the

implementation of the User Datagram Protocol to transmit the data packet (Para 0035). Therefore, it is obvious at the time of the invention was made for one of ordinary skill in the art to incorporate the encryption method of Roberts' invention with Liao's teaching to strengthening the security and integrity of the data transmission.

As per claim 5, see claim 4 rejection.

11.

As per claim 6, Liao and Roberts disclose the method of claim 4. However, Liaos and Roberts do not teach the step of, in the second computer, verifying that the nonce has not previously been received in a previously transmitted data record. Nevertheless, Liaos does teach the nonce verification method during the authentication session setup (Col 9 line 22 to Col 10 line 21). It is obvious at the time of the invention was made for one of ordinary skill in the art that the nonce verification capability is clearly taught. The same method can be implemented to verify the nonce for every packet transmitted.

12. As per claims 10 and 16, Liao discloses a system and a method of securely transmitting a plurality of data records between a client computer and a proxy server (Col 5 lines 13-17, and Col 3 lines 58-67) using an unreliable communication protocol (UDP, Col 6 lines 11-46), comprising the steps of: (1) establishing a reliable connection between the client computer and the proxy

server (Col 3 lines 24-67); (2) exchanging encryption credentials between the client computer and the proxy server over the reliable connection (Col 3 lines 24-67); (5) transmitting the plurality of data records encrypted in step (4) from the client computer to the proxy server using an unreliable communication protocol (UDP, Col 6 lines 11-46). However, Liao does not teach (3) generating a nonce for each of a plurality of data records, wherein each nonce comprises an initialization vector necessary to decrypt a corresponding one of the plurality of data records; (4) using the nonce to encrypt each of the plurality of data records and appending the nonce to each of the plurality of data records; and (6) in the proxy server, decrypting each of the plurality of encrypted data records using a corresponding nonce extracted from each data record and a previously shared encryption key. Nevertheless, Roberts does teach the steps clearly. Roberts teaches the step of generating the random seed (Para 0042) and using the random seed with the master key known by the client to encrypt the message (Para 0043, 0080, and 0081); then transmit the encrypted message with the random seed used to encrypt the message to the client (Para 0082); the client decrypt the message using the known master key with the random seed read from the message (Para 0083). By definition of the nonce, it is also define as a random number or seed in Roberts's invention. Therefore, it is obvious at the time of the invention was made for one of ordinary skill in the art to incorporate the encryption scheme in Roberts' invention with Liao's system to provide a secure and high data integrity transporting method.

13. As per claims 7, 11 and 22, Liao and Roberts discloses the method of claims 1, 10 and 16. However, Liao and Roberts teach the step (6) comprises the step of checking to determine whether each data record received from the client computer is formatted according to a secure unreliable transmission format and, if a particular record is not formatted according to a secure unreliable transmission format, bypassing the decryption using the corresponding nonce. Nevertheless, in Para 0081 of Roberts' invention suggests the implementation of a Secure Parameter Index or other if necessary to ensure compatibility with the encapsulation of the packet for the second computer. Further Roberts teaches the capability to differentiate the encrypted packet and the plain text packet (Para 0034). Therefore, it is obvious at the time of the invention was made for one of ordinary skill in the art that Roberts is explicitly teach the steps to check the data record format using SPI or other parameter at the client computer and response to the data record accordingly.

14. As per claim 12, see claim 10 rejection.

15. As per claim 13, Liao and Roberts discloses the method of claim 10, wherein step (1) is performed using Transmission Control Protocol, and wherein step (5) is performed using User Datagram Protocol (Liao, UDP, Col 6 lines 11-46).

As per claims 14 and 17, Liao and Roberts disclose the method of claims 10 and 16, wherein step (6) is performed using an encryption key previously shared using a reliable communication protocol (Col 6 lines 18-25).

As per claim 15, Liao and Roberts disclose the method of claim 14, wherein the reliable communication protocol is Transmission Control Protocol (Col 6 lines 18-25).

As per claim 18, Liao and Roberts disclose the system of claim 17, wherein the unreliable communication protocol comprises the User Datagram Protocol, and wherein the reliable communication protocol comprises the Transmission Control Protocol (Col 6 lines 18-45).

As per claims 19 and 20, Liao and Roberts discloses the system of claim 16. It is obvious at the time of the invention was made for one of ordinary skill in the art that the communication protocol client function and the communication protocol server function are compatible with the SOCKS communication protocol. It is obvious that Socks supports TLS and UDP (Para 0010 and 0035).

16. As per claim 20, Liao and Roberts discloses the system of claim 16, wherein the communication protocol client function and the communication protocol server functionary compatible with the SSL/TLS communication protocol (See Abstract).

Transport Layer Security (TLS) is also known as Secure Socket Layer (SSL).

As per claim 21, Liao and Roberts disclose the system of claim 16, wherein the second computer comprises a proxy server that forwards decrypted records received from the first computer to a server computer (Col 6 lines 12-30). The link server performs a protocol mapping from Secure Uplink Gateway Protocol to HTTP (See Figure 1, Col 6 line 26).

Conclusion

17. Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (703)-305-8914 or Fax to 703-746-9821.

18. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (703)-305-4393. The fax numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (703)-305-9600.

Linh LD Son

Patent Examiner

AU 2135